DOCUMENT RESUME

ED 459 694 IR 021 053

AUTHOR	Burke, Jennifer
TITLE	Rights, Risks and Responsibilities: Students and the Internet.
INSTITUTION	Southern Regional Education Board, Atlanta, GA.; Southeast and Islands Regional Technology in Education Consortium, Charleston, WV.
SPONS AGENCY	Office of Educational Research and Improvement (ED), Washington, DC.
PUB DATE	2000-05-00
NOTE	9p.; A SREB-SEIR*TEC Publication.
CONTRACT	R302A980001
AVAILABLE FROM	Southern Regional Education Board, 592 10th Street N.W., Atlanta, GA 30318 (Stock no. 00T04, $2 plus $2.50 shipping and handling). Tel: 404-875-9211; Fax: 404-872-1477; Web site: http://www.sreb.org. For full text: http://www.sreb.org/programs/edtech/pubs/_pubstemplate.as p.
PUB TYPE	Reports - Descriptive (141)
EDRS PRICE	MF01/PC01 Plus Postage.
DESCRIPTORS	Computer Uses in Education; Educational Administration; Elementary Secondary Education; *Information Policy; *Internet; *Risk Management; *Safety; *School Policy; Students; *World Wide Web
IDENTIFIERS	*United States (South)

ABSTRACT

Although the Internet can be a powerful learning tool, the materials available can be inaccurate or even dangerous. Students may find themselves the targets of predatory adults, and some may threaten their classmates or others with devices or ideas they find on the Internet. Schools use several methods to ensure that students' use of the Internet is safe and rewarding. These methods include using appropriate-use policies to manage Internet access, supervising students' access to and use of the Internet, and using technology tools to supervise Internet access, each of which is discussed in this publication. Policies, supervision and technical tools are most effective when used together. As more schools and classrooms increase their use of the Internet, parents and other local groups will continue to urge policymakers and administrators to prevent students from accessing inappropriate sites. Having access to different protective approaches, particularly with they can be used together and can be customized to meet local needs, allows teachers and administrators to relax and make the best use of the resources available to students through the World Wide Web. (Contains 10 references.) (AEF)

Reproductions supplied by EDRS are the best that can be made
from the original document.

ED 459 694

Rights, Risks and Responsibilities: Students and the Internet

Jennifer Burke

Southern Regional Education Board
and
Southeast and Islands Regional Technology in Education Consortium (SEIR*TEC)

U.S. DEPARTMENT OF EDUCATION
Office of Educational Research and Improvement
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
X This document has been reproduced as received from the person or organization originating it.
☐ Minor changes have been made to improve reproduction quality.
• Points of view or opinions stated in this document do not necessarily represent official OERI position or policy.

PERMISSION TO REPRODUCE AND DISSEMINATE THIS MATERIAL HAS BEEN GRANTED BY
M.A. Sullivan
TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)
1

IR021053

BEST COPY AVAILABLE

IR

Rights, Risks and Responsibilities:
Students and the Internet

SREB

Jennifer Burke

Student access to the Internet has increased dramatically in the last few years. In 1994, 54 percent of public schools reported that students had some access to the Internet. Today, about 86 percent of schools in the Southeast report that students have Internet access; of those schools, 42 percent report that students can access the Internet in their classrooms. With this increased access comes the possibility of children's exposure to sexually explicit or violent materials on the Internet. Recent news reports have increased awareness about this problem and have prompted demands from parents, teachers and legislators for ways that schools can prevent children from seeing inappropriate or adult materials online. However, protecting students is only one part of the equation. Students, especially those in middle school and high school, are savvy users of the media. Many are experienced in using the Internet but cannot judge which materials are most useful. Schools also need to manage students' access to the Internet to ensure that Internet use supports school and classroom learning goals.

Although the Internet can be a powerful learning tool, the materials available can be inaccurate or even dangerous. Students may find themselves the targets of predatory adults, and some may threaten their classmates or others with devices or ideas they find on the Internet. Many schools use several methods to ensure that students' use of the Internet is safe and rewarding. These methods include:

- **using appropriate-use policies to manage Internet access;**
- **supervising students' access to and use of the Internet; and**
- **using technology tools to supervise Internet access.**

Using appropriate-use policies to manage Internet access

Educators need to develop and consistently reinforce policies for teaching students how best to use the Internet and for defining schools' and students' rights and responsibilities.

May 2000

Southern Regional Education Board

592 10th St. N.W.
Atlanta, GA 30318
(404) 875-9211
www.sreb.org

This is an SREB-SEIR*TEC publication.

The most common method of ensuring that students use the Internet properly is the adoption of an **appropriate-use policy.** Most schools now have appropriate-use policies for Internet use that describe students' and staff members' responsibilities when using school computers. Most appropriate-use policies include the following:

- a description of the instructional philosophies and strategies to be supported by Internet access in schools;
- a statement on the educational uses and advantages of the Internet in a school or district;
- a list of the responsibilities of educators, parents and students regarding Internet use;
- a code of conduct governing student behavior while using the Internet;
- a description of the consequences of violating the appropriate-use policy;
- descriptions of acceptable and unacceptable use of the Internet;
- a disclaimer that absolves the school district, under specific circumstances, from responsibility for materials found on the Internet;
- a reminder to users that the use of computer networks and the Internet is a privilege;
- a statement that the appropriate-use policy complies with state and national rules and regulations regarding telecommunication; and
- a signature form for teachers, parents and students that indicates their intent to abide by the appropriate-use policy.

Kentucky and Louisiana have state laws that require schools and libraries to adopt appropriate-use policies. In most states, however, the decision whether to adopt appropriate-use policies is left to the discretion of local districts and schools. In an effort to ensure that schools' appropriate-use policies are complete and consistent with one another, Virginia has developed guidelines for schools to use in developing the policies. Those who violate acceptable-use policies usually lose their access to the network and can face disciplinary or legal actions.

Supervising students' Internet access and use

Teachers are held accountable for the actions of students assigned to them or students under their supervision. Students say that watchful teachers and librarians — combined with time constraints and pressure to complete assignments — generally prevent them from surfing aimlessly on the Internet or searching for prohibited sites.

Teachers can employ several methods in supervising student use of the Internet. Careful placement of computer stations is the simplest method. For example, computers in a computer lab may be arranged so that a teacher in the center of the room easily can see what's on each screen. Computers in classrooms may be arranged so that the teacher and other students can see the screens, even when students are working on individual projects. Teachers also may limit the available time for Internet access — such as only during a specific class period — or may require students to have adult supervision when using computers. Group projects — in which several students work together on an Internet search — also discourage inappropriate use. Teachers, administrators and other staff members in schools need additional training in supervising students' use of the Internet. In Kentucky, for example, teachers and other adults who supervise students learn how to detect, deter and document inappropriate use; safeguard students' personal privacy; and deal with unsolicited online contact as a school safety issue.

Identifying accurate sources of information is another concern. Most students still are learning to make informed use of research materials. Students familiar with research in traditional libraries expect those sources to be credible and often assume that online information also will be credible. However, while professionals carefully select library materials, materials on the Internet are not evaluated prior to publication. Anyone can publish anything on the Internet and portray it as fact. Internet search engines — including InfoSeek, What-U-Seek, Lycos and Yahoo! — even carry disclaimers that they "shall in no event be liable to anyone for any delays, inaccuracies, errors or omissions." Teachers can help students learn to evaluate carefully the materials on the Internet. Separating fact from fiction or opinion is an important skill for those using today's media.

Students' responsible use of the Internet is reinforced through supervision and instruction in the class or lab. Before students begin a research project, teachers may discuss how to search the Internet effectively and specific situations that may result from student searches. Copyright law, which protects online materials as well as printed ones, may be included in discussions about student bibliographies or plagiarism. Illegal copying of materials, including software or images, is subject to the same disciplinary actions as other network infractions under appropriate-use poli-

cies; punishments may include grade reductions or losses of Internet privileges. It is easy for students accustomed to video games to forget that their inappropriate uses of the Internet may be subject to criminal penalties under state and federal laws. The National School Boards Association has developed a report that describes clearly the issues that administrators should consider when implementing technology in their schools. These issues include protecting students' privacy and enforcing copyright laws. Administrators need to be mindful of their legal responsibilities. In addition to monitoring the materials that students can access on the Internet, teachers and administrators need to monitor what students publish and how students may be using the school network or software. Just as we would not turn a teenager loose with the car unless he or she understood traffic laws, we need to make sure students are aware of ethical use of the Internet and school resources before they get online.

Using technology tools to supervise Internet access

In addition to adopting appropriate-use policies, an increasing number of schools use software products to help screen what students can see on the Internet. **Filtering software** — which prevents access to certain Web sites — can be installed on individual computers or on the school or district network. Some filtering software allows users to select the sites or terms they want to block; others come with blocked sites already selected by the software developer. Many filtering systems also deter inappropriate use of the Internet by allowing school officials to keep track of which Web sites are viewed on school computers. Filtering software, which is available commercially and is relatively inexpensive for school or network use, may alleviate teachers' anxiety about allowing students to search for materials on the Internet. However, filtering software is not 100 percent effective.

States and schools also use **proxy server software on computer networks** to prevent students from accessing forbidden materials on the Internet. This software is installed on the network's main server. It acts as a filter between a Web browser and the main server by intercepting all communication between computers on the local network and the Internet. The proxy server blocks access to certain Web sites (selected either by the programmer or by administrators and teachers) and keeps a record of attempts to access prohibited sites. This software can be customized at the school level to ensure that the school's instructional needs are not inhibited.

Knowing that teachers know which sites they're visiting seems to deter students from seeking out objectionable sites that escape the software's filter. Students even have reported sites that they accidentally had accessed so that those Web sites could be blocked. In Tennessee, officials say that Internet use has increased since the

Kentucky's General Assembly in 1998 enacted Senate Bill 230, which requires schools to prevent sexually explicit materials from being transmitted via educational technology systems. To comply with SB 230, the Kentucky Department of Education installed a *proxy server software* on the statewide network. The software creates checkpoints on each school's network, saves copies of frequently accessed sites, and blocks selected Internet files. Schools and teachers can decide which sites should be blocked.

November 1998 installation of filtering software on the statewide network, ConnecTEN. One possible explanation is that the software made teachers feel more comfortable about allowing children to use the Internet.

However, technology that restricts access to certain sites is not foolproof and can lull teachers and parents into a false sense of security. Photographs and other graphics, which often are not filtered, may be placed on Web sites with innocent-sounding names. Use of filtering software does not excuse school officials from their responsibility for supervising students' use of the Internet. Other problems are that software technicians — rather than educators — decide how to filter or block sites and that the criteria used by software companies for blocking sites generally are not made available. As a result, schools do not know whether filters inadvertently have blocked Web sites that have high educational value. School districts should not expect technology, such as software, to replace planning and training for teachers and students who use the Internet.

Filtered service providers are another way to manage student access to the Internet. In the last few years several companies that provide Internet access have built filtering software into their network systems. These companies say that their systems do a better job than traditional filtering software of preventing computer-savvy youngsters from getting around the filters. Although most of these companies target families who use the Internet at home, several now market themselves to schools. Schools that do not already receive Internet services through a district or state education network may choose to access the Internet through these companies. Users of these services cannot customize the list of blocked sites, however, because the Internet service provider makes those decisions.

Educational portals (access points to preselected Internet searches and online curricula) give students access only to certain Web sites that are appropriate for their use. Rather than filtering out inappropriate sites, these products provide a collection

of appropriate materials, including full-text articles, suggestions for structured class activities, and links to educational Internet sites that have been evaluated and selected. Searches in these systems retrieve only materials that appear on a preselected list of Web sites. The service provider has evaluated these educational materials, which usually are organized by subject for easy use by students and teachers. Individual schools subscribe to these services.

Conclusion

Even though individual schools and districts are taking steps to ensure the safety of students who use the Internet, some elected officials are working to require such actions. In the last year, the legislatures in Arkansas, North Carolina, Tennessee and Texas considered legislation that would require schools and public libraries to have acceptable-use policies and software to block and filter Web sites. A bill introduced during the 1999 session of the North Carolina General Assembly would have required libraries to limit access by people younger than 18 to certain kinds of content on the Internet. Such legislation raises potentially difficult issues for public libraries and college and university libraries. Laws in effect in 1999 in both Kentucky and Louisiana require schools, school districts and libraries to use filtering software, other technology or appropriate-use policies to protect schoolchildren from inappropriate or dangerous material either on the Internet or via e-mail.

Policies, supervision and technical tools are most effective when used together. It is important not only to establish policies but also to enforce them consistently and to respond to abuses of the school network. For example, filtering software on Tennessee's network enables officials to track which computers and students are involved in incidents. Law enforcement officers can interview students who have engaged in illegal activities. Involvement by law enforcement agencies in support of school principals and superintendents reinforces to students the importance of responsible use and demonstrates that Tennessee schools take their appropriate-use policies seriously.

As more schools and classrooms increase their use of the Internet, parents and other local groups will continue to urge policy-makers and administrators to prevent students from accessing inappropriate sites. Schools and districts that have not adopted at least one measure to control access likely will do so. Fortunately, the tools to help them provide a safe gateway to the Internet are reasonably priced. Having access to different protective approaches, particularly when they can be used together and can be customized to meet local needs, allows teachers and administrators to relax and make the best use of the resources available to students through the World Wide Web.

Additional resources

Aftab, Parry. *The Parent's Guide to the Internet and Protecting Children in Cyberspace.* New York: McGraw-Hill, 2000.

American Association of School Administrators, sample Internet acceptable-use policies: www.aasa.org/issues/techplans/planstc.htm.

American Library Association Resources for Parents, Teens and Kids: http://ala8.ala.org/parents/.

Evaluating the Content of Web Sites: www-comdev.ag.ohio-state.edu/eetap/publications.htm.

GetNetWise: www.getnetwise.org/.

Learning Space Online Teacher Network: www.learningspace.org/.

National Parent Information Network: www.npin.org/.

National School Boards Association. *Legal Issues and Education Technology: A School Leader's Guide.* Alexandria, Va.: National School Boards Association, 1999.

University of Oklahoma Department of Public Safety, slide show to help teach children about safe Internet use: www.ou.edu/oupd/kidsafe/start.htm.

U.S. Department of Justice: www.usdoj.gov/kidspage/do-dont/kidinternet.htm.

The Southern Regional Education Board is a partner in the SouthEast and Islands Regional Technology in Education Consortium, one of six U.S. Department of Education regional technology consortia. SEIR*TEC promotes the use of technology to improve teaching and learning, with emphasis on benefiting traditionally underserved populations.

This document is based on research supported in part by the Office of Educational Research and Improvement, U.S. Department of Education, under CFDA 84.302A, grant number R302A980001. Its contents do not necessarily reflect the views of OERI, the U.S. Department of Education or any other agency of the U.S. government.

For more information contact Jennifer Burke, SREB staff associate, at 404-875-9211 or via e-mail at jburke@sreb.org.